Case Study
Digital Forensics and Incident Response
+ Strategic Communications

Integrated Incident Response

Customer: DP World
Industry: Logistics
Services: DFIR and Strategic Communications

Overview

- On 10 November 2023, DP World (DPW) Australia detected unauthorised access to the company's Australian corporate network.
- To contain the incident, the DPW team isolated the network from the internet, stalling port operations.
- Once the network was isolated, DPW experienced understandable pressure to get ports reopened and resume the flow of trade.
- The business managed significant interest from media, consumer, private industry and government stakeholders.

Outcome

- Rapid reaction to contain breach, with first CyberCX team on the incident in under one hour.
- Ports recommenced operation within two business days of first detection, and 100% of backlog – or some 30,137 containers – were cleared seven days after ports recommenced.
- Feedback from key stakeholders, including government, that DP World's communications response was industry leading.

DP World

DP World is Australia's leading provider of end-to-end supply chain logistics solutions, responsible for moving more than 40% of the country's maritime freight.

Through its Terminals and industrial Logistical Parks strategically located in Brisbane, Sydney, Melbourne and Fremantle, DP World offers a comprehensive range of products and services to enhance the efficiency of cargo movement through seamless rail, road and sea.

The incident

On Friday, 10 November 2023, DP World (DPW) Australia detected unauthorised access to the company's Australian corporate network.

To contain the incident, the DPW team made the decision to isolate the network from the internet. While this successfully contained the incident, it also halted port operations, causing a backlog of some 30,137 containers.

The DPW investigation confirmed the incident was confined to the Australian market, nor was ransomware found or deployed within the network. However, some of its files were accessed by the unauthorised third party and a small amount of data – comprising of personal information from current and past employees – was exfiltrated.

The solution

Digital Forensics and Incident Response

To support DPW's technical response, the business engaged CyberCX's Digital Forensics and Incident Response (DFIR) team, who immediately commenced analysis of the affected servers to scope the incident. Throughout the investigation, the DFIR team worked alongside the technical and subject matter experts at DPW to track the activities of the threat actor through corporate systems.

CyberCX was able to attribute the activity to a particular threat actor which dictated the response and containment actions and associated remedial advice.

Key deliverables included:

- Working with DPW to chart a pathway to end network isolation and recommence operations;
- Ascertaining how the threat actor accessed the environment;
- Discovering which systems and accounts the threat actor had accessed;
- Confirming which credentials needed to be changed; and
- Identifying what data the threat actor exfiltrated prior to eviction.

Strategic communications advisory

CyberCX's Strategic and Crisis Communications team were deployed alongside the technical team to DPW's Australian head office.

CyberCX worked to familiarise the DPW Corporate Affairs team with the unique challenges of communicating to their high risk and high needs audiences about a cyber incident, including:

- Proactively bringing a diverse external stakeholder group on the disclosure journey;
- Co-designing a go-public and ongoing communications approach that aligned all internal stakeholders, from the boardroom to the help desk; and
- Meeting legal requirements across different jurisdictions, contractual obligations with key business partners, and avoiding the creation of undue legal risk for the organisation.

Key deliverables included:

- Communications strategy preparation, including disclosure preparation and support;
- Mapping and coordination of key external stakeholder briefings;
- Briefings to key internal stakeholders;
- Key statement and Q&A drafting; and
- Media briefing, liaison, and monitoring

The outcome

By partnering with CyberCX, DP World was able to effectively identify, protect, detect, respond to, and recover from the cyber incident.

Key outcomes included:

- CyberCX deploying all necessary resources both on-site and remotely as required, with the first team embedded on the incident in under one hour.
- Limited disruption with ports back in operation within two business days.
- Feedback from key stakeholders that DPW's communication and stakeholder management approach was industry-leading, including in government commentary.

"CyberCX was instrumental in helping us manage and recover from the cyber incident in November 2023. Their team was on-site within the hour, working alongside ours to quickly contain the breach and assess the impact. They brought not just technical expertise, but also practical guidance and strong communications support — which was critical as we navigated high levels of scrutiny from stakeholders, regulators and the public.

With their support, we had ports operating again within two business days and cleared the container backlog in under a week. Their response helped us protect our operations and maintain trust where it mattered most. We appreciate their speed, clarity and partnership throughout the incident."

Garran Jones, Senior Vice President – Information Technology – APAC, DP World

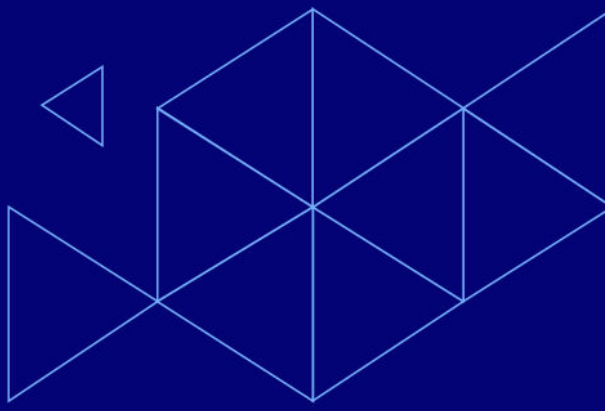
About CyberCX

CyberCX is the leading provider of professional cyber security and cloud services across Australia and New Zealand. With a workforce of over 1,400 professionals, we are a trusted partner to private and public sector organisations helping our customers confidently manage cyber risk, respond to incidents and build resilience in an increasingly complex and challenging threat environment.

Through our end-to-end range of cyber and cloud capabilities, CyberCX empowers our customers to securely accelerate opportunities in the digital economy.

Our expertise is represented across 12 cyber security and cloud practices:

- Strategy & Consulting
- Governance, Risk & Compliance
- Security Testing & Assurance
- Privacy Advisory
- Identity & Access Management
- Network & Infrastructure Solutions
- Cloud Security & Solutions
- Managed Security Services
- Cyber Capability, Training & Education
- Cyber Intelligence
- Digital Forensics & Incident Response
- Cyber Strategic Communications



Contact us to find out how CyberCX can boost the cyber security skills of your entire organisation.

cybercx.com.au

1300 031 274

CyberCX